UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,385	06/19/2002	Tobias Martin	520.1007	3809

7278 7590 02/05/2007

DARBY & DARBY P.C.
P. O. BOX 5257
NEW YORK, NY 10150-5257

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/049,385	MARTIN ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-15* is/are pending in the application.

4a) Of the above claim(s) *3 and 4* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 10 November 2006. By this response, Claims 5 and 6 have been amended. New Claims 7-15 have been added. No claims have been canceled. Claims 3 and 4 were previously withdrawn from further consideration as directed to a nonelected invention. Claims 5-15 are currently under examination in the present application.

Response to Arguments

2. Applicant's arguments filed 10 November 2006 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 5 and 6 under 35 U.S.C. 101 as directed to non-statutory subject matter, Applicant argues that establishment of a common key as claimed is a concrete, tangible, and useful result (see page 11 of the present response). However, as noted in the previous Office action, although generation of a key is concrete and useful, it is **not tangible**. A key is a piece of data that is merely a number or sequence of bits, which, in and of itself, is not a tangible object. The Examiner notes that although Claim 5 has been amended to include that the claimed method is "for transmitting messages over a communication channel" and that the key is "useable for transmitting messages over a communication channel" (page 11 of the present response), these limitations merely recite an intended use for the claimed method

without actually providing steps for realizing that use. That is, although the key can be used for transmitting messages, which the Examiner agrees is a concrete, tangible, and useful result, the claim does not set forth any steps in which a transmission of a message actually occurs. Therefore, as noted above and in the previous Office action, although establishment of a key is a concrete and useful result, it is **not a tangible result**.

The Examiner further notes that new Claims 7-14 are also non-statutory for similar reasons, as set forth below. The Examiner additionally notes that, in contrast, new Claim 15 is directed to statutory subject matter, because the claim further recites limitations of encrypting, transmitting, and decrypting a message. This realizes a practical application of the claimed abstract idea (i.e. algorithm) and therefore the method constitutes statutory subject matter.

Regarding the rejection of Claim 5 under 35 U.S.C. 112, second paragraph, as indefinite, it is noted that the features upon which applicant relies are not recited in the rejected claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Specifically, Applicant first argues that "it is not necessary for each subscriber Tj ($j \neq 1$) to have direct access to the random number z1" (see page 12 of the present response); however, from the claimed language regarding the assignment $k:= h (z1, g^{z2}, ..., g^{zn})$, it appears that the claim does, in fact, require direct access to the random number z1. Further, although Applicant argues that each subscriber is able to decrypt the encrypted random number z1 because $k^{1j} = k^{j1}$

(page 13 of the present response), such a definition of the properties of the transmission key is **not recited** in Claim 5. In the same paragraph, Applicant argues that each subscriber is able to calculate a common key according to the above-noted assignment k because h "has the property that it is symmetrical in its arguments". However, the Examiner notes that this does not appear to follow logically, and the Examiner further notes that each of the subscribers Tj does not, as claimed, appear to have access to all of the required parameters z1, g^{z2}, ..., g^{zn}.

Further, with reference to the example provided in the specification, Applicant argues that T_2 has $(g^{z3})^{z1}$ from M_{13} and T_3 has $(g^{z2})^{z1}$ from M_{12} (see the paragraph spanning pages 13-14 of the present response); however, the Examiner notes that **nowhere is it claimed** that T_2 receives M_{13} or that T_3 receives M_{12}. Additionally, the claim requires that, to calculate the assignment k:= h (z1, g^{z2}, ..., g^{zn}), each of the subscribers Tj specifically use the parameters g^{z2}, ..., g^{zn}, and not $(g^{zj})^{z1}$ as Applicant asserts that the subscribers possess. The Examiner also notes that the **claim does not explicitly state** that the subscribers receive each $(g^{zj})^{z1}$ as Applicant asserts. The claim only states that each subscriber Tj, $j \neq 1$, is sent a message M_{1j} as defined in the claim.

Regarding the rejection of Claim 6 under 35 U.S.C. 112, second paragraph, as indefinite, Applicant states that Claim 6 does not recite a variable "k^{j1n}" which Applicant asserts was the cause of the rejection of Claim 6 (page 14 of the present response). However, the Examiner notes that such a variable was not referred to, and instead Claim 6 was rejected partly because the variable "k^{j1}" was not defined anywhere in Claim 5 or Claim 6. The Examiner believes that this is still the case. Although Applicant

states that "$k^{1j} = k^{j1}$" was defined in Claim 5, the Examiner respectfully disagrees. Although k^{1j} is defined in Claim 5, k^{j1} does not appear to be defined or used anywhere in Claim 5, contrary to Applicant's assertion.

The Examiner further notes that new Claims 7-15 are also rendered indefinite for similar reasons as Claim 5, as set forth below.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Specification

3. The objection to the disclosure for informalities is withdrawn in light of the amendments to the specification. Applicant's cooperation is again requested in correcting any further errors of which applicant may become aware in the specification.

Claim Objections

4. Claims 13 and 14 are objected to because of the following informalities:

In Claim 13, it appears that, in lines 17 and 20 of the claim, "subscribes" is intended to read "subscribers".

In Claim 14, it appears that "wherein" is instead intended to read "whereby", noting that the specification describes that the maximum number of transmission rounds is a consequent result of the method (see paragraph 0025).

Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 5-14 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, Claims 5-14 are directed to methods for establishing a key. The result of those methods is the determination or computation of a common key, which produces neither a physical transformation nor a concrete, tangible, and useful result. Although the determination of an encryption key is likely to be both concrete and useful, it is not a tangible result. Similarly, determination of such a key does not cause any physical transformation. Therefore, the methods are directed only to an abstract idea, which is non-statutory subject matter. See MPEP § 2106 IV.B.2(b).

Claim Rejections - 35 USC § 112

7. Although some issues of indefiniteness have been remedied by the amendments to the claims, other issues remain, as detailed above, and the new claims raise further issues of indefiniteness. Therefore, the claims remain rejected as set forth below.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 5-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites the limitation "determining a common key k by each subscriber Tj using an assignment k := h (z1, g^{z2}, ..., g^{zn})". The Examiner notes the correspondence between the values Nj, and the g^{z2} ... g^{zn}. However, it is not clear from the claims how each subscriber Tj ($j \neq 1$) has access to the values g^{z2} ... g^{zn}, as it appears that each subscriber Tj only has access to its own value g^{zj}, but not those of the other subscribers. Further, it is not clear how the subscribers Tj ($j \neq 1$) have access to the random number z1. Although z1 is sent to each subscriber from the first subscriber T1, it is sent encrypted with transmission key k^{1j}. It is not clear how each subscriber Tj ($j \neq 1$) has access to the transmission key k^{1j} since the key depends on both Nj, which subscriber Tj possesses (having generated that value in the first claimed step), and z1, which subscriber Tj does not appear to possess, having received only the encrypted form of z1. That is, it appears that to decrypt the value z1, the subscribers Tj ($j \neq 1$) must already have access to z1 in order to generate the key for decryption. The above inconsistencies render the claims indefinite, as it appears that steps are missing which would provide for the receipt by each subscriber Tj of the values g^{z2} ... g^{zn} (except for g^{zj}) and also for the receipt or calculation of the symmetric decryption key that would allow decryption of the encrypted random number z1. The Examiner notes that it is not

clear from the specification exactly how the omission of such steps would be remedied, and therefore it is not possible to fully determine the scope of the claims for interpretation of the prior art, as noted below.

Claim 6 recites the variable "k^{j1}"; however, the variable is not defined or used anywhere in either Claim 5 or Claim 6.

Claim 7 recites the limitation "each of the subscribers Tj computing a common key k according to an assignment k := h (z1, g^{z2}, ..., g^{zn})". As described above in reference to Claim 5, it is not clear from the claims how each subscriber Tj ($j \neq 1$) has access to the values g^{z2} ... g^{zn}, as it appears that each subscriber Tj only has access to its own value g^{zj}, but not those of the other subscribers. Further, it is not clear how the subscribers Tj ($j \neq 1$) have access to the random number z1. Although z1 is sent to each subscriber from the first subscriber T1, it is sent encrypted with transmission key k^{1j}. It is not clear how each subscriber Tj ($j \neq 1$) has access to the transmission key k^{1j} since the key depends on both Nj, which subscriber Tj possesses (having generated that value in the first claimed step), and z1, which subscriber Tj does not appear to possess, having received only the encrypted form of z1. That is, it appears that to decrypt the value z1, the subscribers Tj ($j \neq 1$) must already have access to z1 in order to generate the key for decryption. The above inconsistencies render the claims indefinite, as it appears that steps are missing which would provide for the receipt by each subscriber Tj of the values g^{z2} ... g^{zn} (except for g^{zj}) and also for the receipt or calculation of the symmetric decryption key that would allow decryption of the encrypted random number z1. The Examiner notes that it is not clear from the specification

exactly how the omission of such steps would be remedied, and therefore it is not possible to fully determine the scope of the claims for interpretation of the prior art, as noted below.

Claim 7 further recites the limitations "the respective first message" in line 7; "the received respective first message N_j" in line 9; "the transmission key k^{1j}" in line 12; and "the encrypted second message M_{1j}" in line 13. There is insufficient antecedent basis for these limitations, because it is not explicit and clear to which of the multiple first messages, transmission keys, and second messages these limitations refer, or if they are intended to refer to each (or all) of the first messages, each (or all) of the transmission keys, and each (or all) of the second messages.

Claim 8 recites the limitation "the respective random number zj"; however, it is not clear to which random number this is intended to refer, or if it is intended to refer to each or all of the random numbers.

Claim 11 recites the variable "k^{j1}"; however, the variable is not defined or used anywhere in either Claim 7 or Claim 11.

Claim 13, similarly to Claims 5 and 7, recites the limitation "each of the subscribers Tj computing a common key k according to an assignment k := h (z1, g^{z2}, ..., g^{zn})". As described above in reference to Claim 5, it is not clear from the claims how each subscriber Tj ($j \neq 1$) has access to the values g^{z2} ... g^{zn}, as it appears that each subscriber Tj only has access to its own value g^{zj}, but not those of the other subscribers. Further, it is not clear how the subscribers Tj ($j \neq 1$) have access to the random number z1. Although z1 is sent to each subscriber from the first subscriber T1, it is sent

encrypted with transmission key k^{1j}. It is not clear how each subscriber Tj ($j \neq 1$) has access to the transmission key k^{1j} since the key depends on both Nj, which subscriber Tj possesses (having generated that value in the first claimed step), and z1, which subscriber Tj does not appear to possess, having received only the encrypted form of z1. That is, it appears that to decrypt the value z1, the subscribers Tj ($j \neq 1$) must already have access to z1 in order to generate the key for decryption. The above inconsistencies render the claims indefinite, as it appears that steps are missing which would provide for the receipt by each subscriber Tj of the values g^{z2} ... g^{zn} (except for g^{zj}) and also for the receipt or calculation of the symmetric decryption key that would allow decryption of the encrypted random number z1. The Examiner notes that it is not clear from the specification exactly how the omission of such steps would be remedied, and therefore it is not possible to fully determine the scope of the claims for interpretation of the prior art, as noted below.

Claim 13 further recites the limitations "the respective first message" in line 8; "the received respective first message N_j" in line 11; "the transmission key k^{1j}" in line 14; "the encrypted second message M_{1j}" in line 15; and "the respective memory" in line 18. There is insufficient antecedent basis for these limitations, because it is not explicit and clear to which of the multiple first messages, transmission keys, second messages, and memories these limitations refer, or if they are intended to refer to each (or all) of the first messages, each (or all) of the transmission keys, each (or all) of the second messages, and each (or all) of the memories.

Examiner's Note

10. Because the claims are rendered indefinite by the several issues detailed above in reference to the rejection under 35 U.S.C. 112, second paragraph, and the amendments to the claims have not overcome those issues, it has still not been possible to determine the scope of the claims, and therefore it has still not been possible to search fully the prior art for the claimed subject matter in order to make a determination regarding the patentability of the claims with respect to novelty under 35 U.S.C. 102 and non-obviousness under 35 U.S.C. 103. Further search has been made to the extent possible.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER